FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Martin Čtrnáctý
Oponent práce:	Ing. Karel Hynek
Název práce:	Softwarový modul pro rozpoznání VPN v síťovém provozu
Obor:	Počítačové systémy a sítě

Datum vytvoření: 3. 6. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Zadání bylo splněno v celém rozsahu.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*75 (C)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Text práce je napsaný srozumitelně. Ačkoliv mám pocit, že část 1.4 zařazená pod rešerši patří spíše do kapitoly Analýza a návrh považuji členění práce za logické a nemám k němu žádných závažných výhrad. Práce obsahuje pouze 14 citací a některým pasážím zdroj vyloženě chybí. Během čtení jsem nezaznamenal žádné typografické chyby a překlepy. Text místy předává čtenářovi jen kusé informace bez dalšího vysvětlování. Například důvod použití "luamodule" se dozvíme, ale jen z části. Práce rovněž zamlčuje určité nastavovací konstanty, které je třeba dohledat přímo v kódu. Celkově text hodnotím jako průměrný.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*85 (B)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů

Komentář:
Autor navrhl a implementoval několik detekčních metod VPN spojení, které následně porovnává. Detekční metody jsou jsou navržené rozumně, zdrojový kód je srozumitelný, avšak místy chybí komentáře. Text práce sice částečně popisuje i zdrojový kód, nicméně při samotném prohlížení příloh bych uvítal také elektronickou formu dokumentace (např. v Doxygenu). Značným způsobem by se tím zvýšil vhled do implementovaných detektorů.

Experimenty s deterministickými metodami jsou navrženy dobře a nemám pochybnosti o jejich případné reprodukovatelnosti. Měření přesnosti detektoru, který využívá strojové učení ale bohužel vůbec neřeší problém statistického výběru a myslím, že by bylo možné ho provést lépe.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

4. Hodnocení výsledků, jejich využitelnost	*95 (A)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Práce popisuje návrh, implementaci a následné srovnání detekčních metod VPN tunelů. Ačkoliv mě mrzí, že i deterministické algoritmy nebyly odzkoušené i na reálných datech z páteřní sítě, představené výsledky budou základem dalšího výzkumu detekce VPN spojení.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

V popisu paketové detekce píšete že spojení je úspěšně detekováno, pokud proběhne odeslání určitého množství zpráv typu "data". Kolik přesně takových zpráv se musí odeslat, aby bylo spojení označeno jako VPN tunel?

Proč jste nepoužil pro anotaci dat ze sítě CESNET2 vámi implementovaný detektor VPN spojení, který využívá analýzu paketů?

Která z vámi vybraných charakteristik je nejvíce důležitá pro detekci VPN spojení?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Celkové hodnocení	*85 (B)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Student odvedl velké množství práce při analýze možnostech detekce VPN tunelů a následné implementaci několika detekčních algoritmů v jazyce python. Samotný text je bohužel nejslabší stránkou a vynechává některé základní informace, které by tam měly být. Pro plnou využitelnost práce chybí porovnání detekčních metod na datech ze sítě CESNET2. I přes výše zmíněné nedostatky doporučuji práci k obhajobě a hodnotím ji známkou B.

Podpis oponenta práce: